

INVESTIGATION INTO OPEN-SOURCE CYBER THREAT INTELLIGENCE SOLUTIONS FOR THE HEALTHCARE SECTOR

Lee Canning (2116294), Digital Health and Care Wales



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

RESEARCH CONTEXT



DHCW provide critical digital services for healthcare [1].



Protecting patient data.



Constant challenge to secure infrastructure.



Attacks: Wannacry (2017), Synnovis (2024).



Analysis into potential OSCTI solutions for DHCW.



Leverage Cybersecurity knowledge.



RESEARCH PROBLEM

“How can the integration of Open-Source Cyber Threat Intelligence systems enhance patient data protection and mitigate the risks to current healthcare security frameworks posed by globally emerging cyber threats?”

- Critical requirement to implement OSCTI.
- Complement existing security portfolio.
- Threat actors, threat landscape.



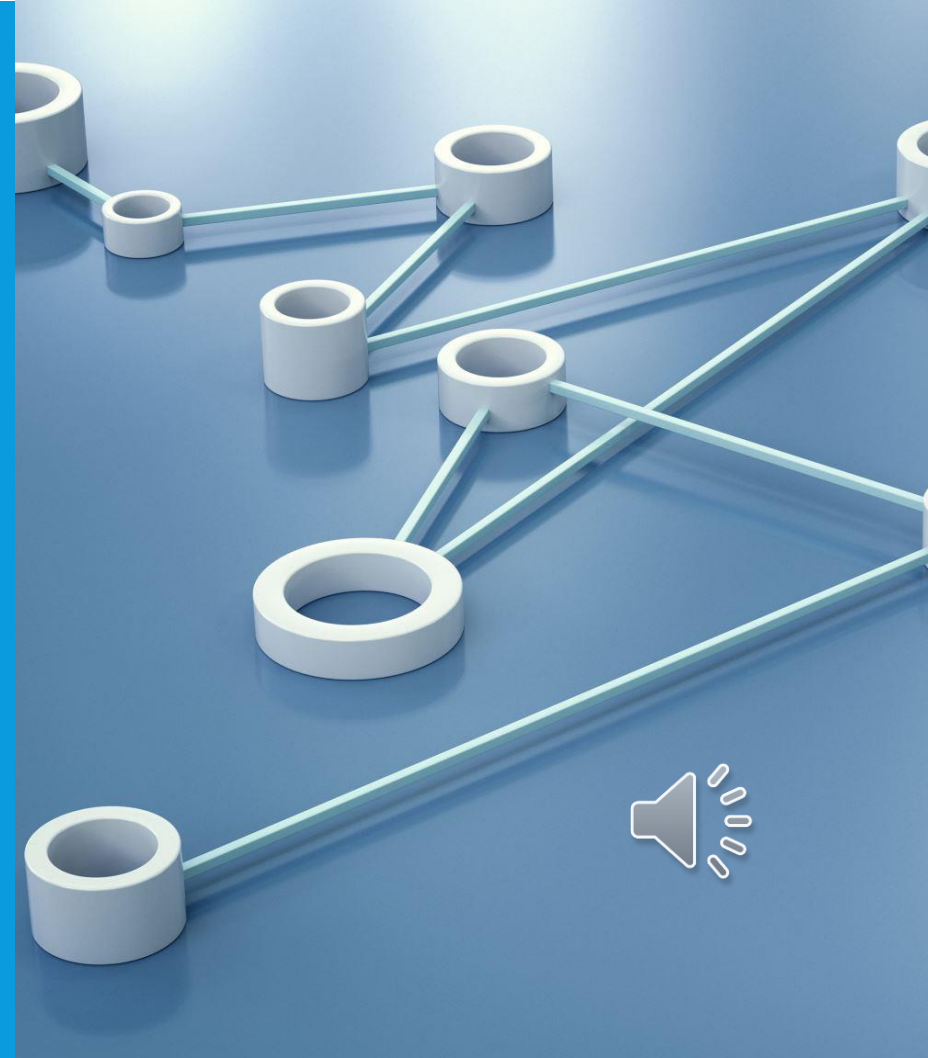
RESEARCH AIM & OBJECTIVES

AIM

- To conduct in-depth analysis and experimentation to recommend an appropriate OSCTI solution that will enhance DHCW's cyber resilience.

OBJECTIVES

- Conduct research into OSCTI trends and key features.
- Identify vulnerabilities in organisational infrastructure.
- Conduct experiment on existing OSCTI solutions.
- Recommend a suitable solution.



LITERATURE REVIEW



CYBERSECURITY
ENABLES DHCW TO
MEET OBJECTIVES [4].



ANTIVIRUS,
FIREWALLS, VPN



CTI/OSCTI GATHERS,
ANALYSES THREAT
DATA.



NEWS FEEDS, SOCIAL
MEDIA, DEEP/DARK
WEB, OSI STREAMS [5].



TOOLS TO GENERATE
AND DISTRIBUTE
THREAT INFORMATION.



LITERATURE REVIEW [CONTINUED]



Threat Intelligence Feeds.



www.virustotal.com, www.cisa.gov/ais.



Types of Threat Intelligence

Operational

Tactical

Strategic



LITERATURE REVIEW [CONTINUED]

- Microsoft Defender Threat Intelligence (MDTI)
- Malware Information Sharing Platform (MISP)
- TheHive

Tool	Licence	Targeted Threats	Key Features	Integration Capabilities
Microsoft Defender Threat Intelligence	Commercial (Free version available)	Malware, phishing, ransomware	Advanced threat hunting, threat intelligence enrichment.	Seamlessly with Microsoft Defender products. Limited for organizations using a mix of security software.
MISP (Malware Information Sharing Platform)	Open-Source	Malware, IOCs, threat actors	Centralized repository, customisable taxonomies, integration.	Highly customizable and uitable for organizations with diverse security portfolios.
OpenCTI	Open-Source	General cyber threats	Graph-based visualisation, data enrichment, API integration	Flexible and customisable API that can be integrated with various security tools and platforms.
TheHive	Open-Source	Security incidents	Incident response management, case managemen.	Easily integrates with other security tools and platforms, ideal for organisations that need a centrally managed security platform.



RESEARCH METHODOLOGIES

Mixed-methods approach

- Quantitative data: Number of un/successful attacks.
- Qualitative data: Tactics, motivation.
- Utilise highly reliable and valid data

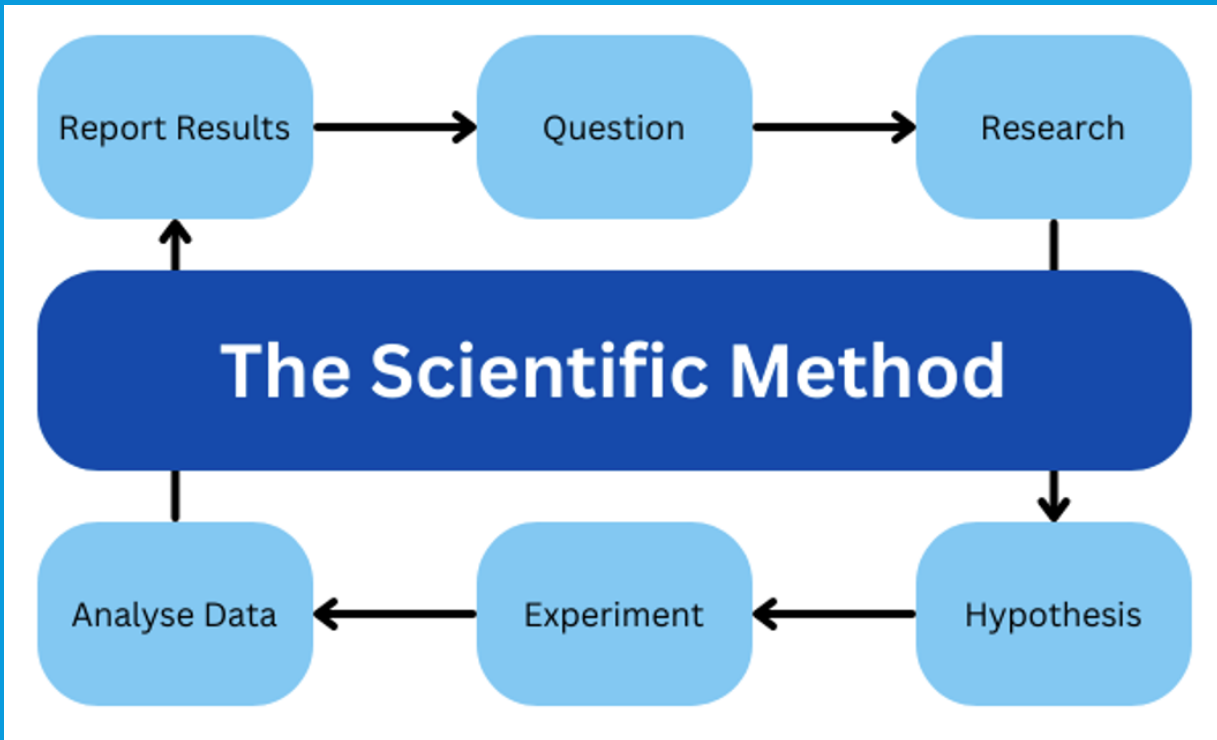
Strategies

- Literature review
- Case Study
- Experiment



DEVELOPMENT METHODOLOGIES

Scientific Method



Hypothesis

- H_0
Implementing OSCTI software 'X' within the DHCW network will not provide any added security benefits.
- H_1
Implementing an OSCTI software 'X' will provide an added layer of security to safeguard networks and patient data.



RESOURCES/MATERIALS

Hardware

- Laptop
- DCHW Network

Software

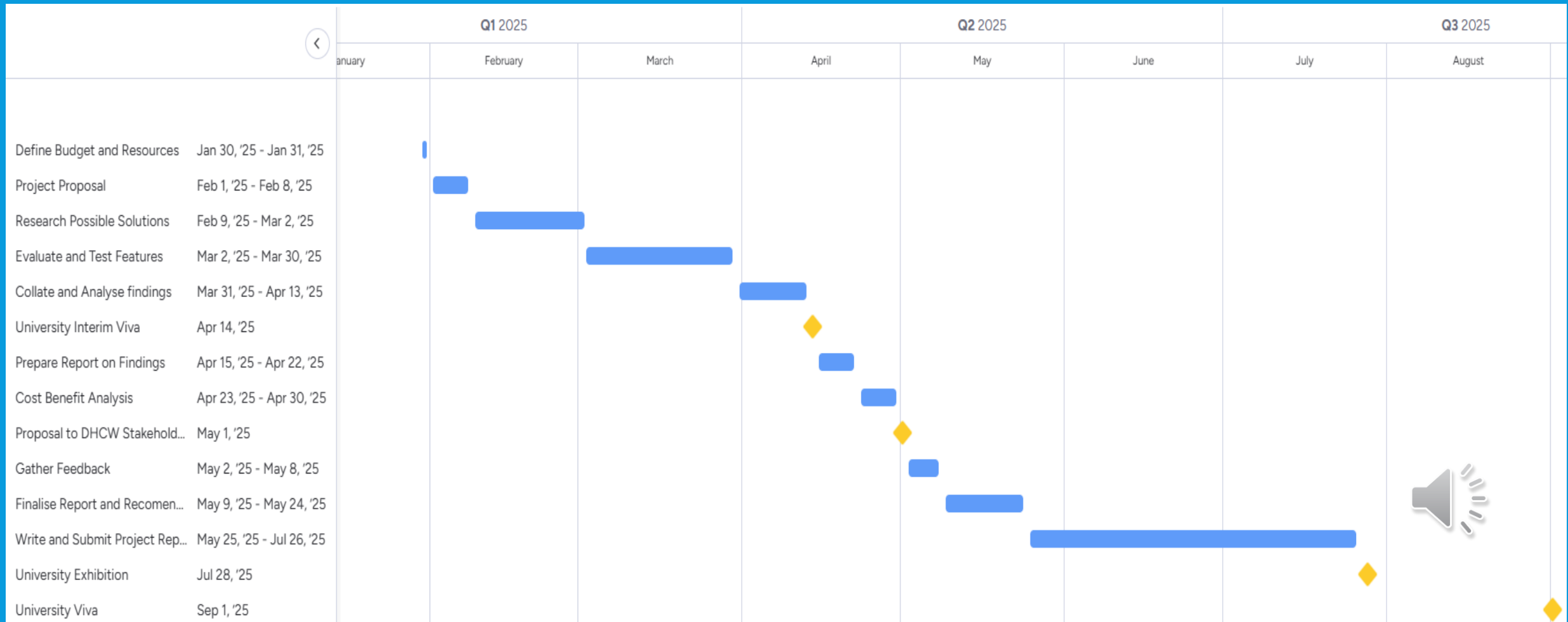
- MSDTI, MISP, TheHive
- Web Browser
 - Chrome, Edge, Tor
- MS Excel, Tableau

Human Resources

- DHCW Cybersecurity
- DHCW Cyber Resilience
- Networking



PROJECT PLAN



REFERENCES

- [1] DHCW, "Digital Health and Care Wales Organisational Strategy 2024 - 2030," 2024. [Online]. Available: <https://dhcw.nhs.wales/about-us/key-documents/strategies/organisational-strategy-2024-2030/#about>. [Accessed 01 August 2024].
- [4] DHCW, "Cyber Security Three Year Plan," Digital Health and Care Wales, Cardiff, UK, 2022.
- [5] "Threat Intelligence in Cybersecurity," EC-Council, 7 March 2024. [Online]. Available: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/what-is-cyber-threat-intelligence/#:~:text=Cyber%20Intelligence%20is%20the%20knowledge,%2C%20their%20motive%2C%20and%20capabilities..> [Accessed 03 August 2024].



ONLINE LINK

The presentation can be viewed online, at:
<https://youtu.be/41Z-1en59gg>

